

REMARKS

Applicants have carefully reviewed the Office Action dated January 23, 2006, the cited references, and the reasons for rejection of the claims. Applicants respectfully submit that, based on this Response, this application is in condition for full allowance and respectfully request such allowance.

The above amendments to the specification are submitted to remove various typographical informalities. Applicants respectfully submit that these changes are respectfully asserted not to introduce new matter, and their entry is respectfully requested.

Review of the References

Blakeley (U.S. Patent No. 5,832,211) relates to a network system server that provides password synchronization between a main data store and a plurality of secondary data stores so that a user is able to maintain a single, unique password among the plurality of secondary data stores. Blakeley uses a password synchronization server to store user names and plain-text passwords securely and to respond to requests from secondary data stores for their retrieval. The passwords are sent to the secondary data stores using encryption that is decipherable by the secondary data stores.

Blakeley does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information.

Mehring (U.S. Patent No. 6,609,115) relates to a method of allowing a remote system user to request multiple software applications using a single log-in. Although the remote user is only required to log-in once, the user information is submitted to the policy server every time the remote user logs-in to a different web server.

Like Blakeley, Mehring does not teach or suggest migrating data from a source datastore to a target datastore, and does not address the problem of migrating from one vendor's proprietary encryption scheme to another vendor's product without having every user re-enter their security information.

Response to Rejections under Section 103

In the Office Action dated January 23, 2006, Claims 1-24 were rejected under 35 U.S.C. Section 103(a) as being unpatentable over Blakely (U.S. Patent No. 5,832,211), and further in view of Mehring (U.S. Patent No. 6,609,115).

I. Blakely does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that locates a corresponding identification in a target datastore and determines whether the target datastore includes a password associated with the identification.

Claim 1 recites, “A method for migrating from a source user authenticator ... to a target user authenticator ... comprising ... Locate the corresponding identification in the target datastore and determine whether the target datastore includes a password associated with the identification.”

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, Applicants are unable to find such a teaching in Blakely. The section of Blakely cited in support of this suggestion (Col. 11, lines 44-55) describes the requirements met by the password synchronization function. The requirements do not include locating a corresponding identification in their target datastore and determining whether their datastores include a password associated with the identification. It is not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because they are networked with the main data store. Their datastores are configured to be propagated immediately with any changes to passwords in the DCE datastore. Col. 11, lines 27-32 of Blakely states:

... synchronization causes passwords changed by DCE users to be propagated as plaintext passwords **to any** other foreign registry configured to receive such changes. **Propagation is immediate**, with results saved for retry, as necessary, should communications with the foreign registries be broken. (Emphasis added by Applicants.)

Therefore, no determination is made by the foreign registries. They simply receive any changes made to the DCE passwords.

More importantly, simply propagating passwords from one datastore to another is not possible when migrating from one vendor's proprietary database schema to another vendor's

product. While one could always simply change out the authentication system and have every user re-register to provide new security information, this involves substantial coordination including safeguards that the authorized user is the one providing the new information. It also causes significant additional effort by the end users, while a more transparent migration reduces end user frustration. Finally, in a simple world one could replicate or transform the security datastore to a datastore for the new system, porting the information across all at once and having it available for the new authenticator to use. However, as discussed above, the custom nature of some of the schema and the various encryption efforts make this task highly challenging to impossible for some migrations.

In response to these difficulties, the present application discloses a desirable feature in a security migration to port user data out of the proprietary and/or encrypted datastore of the old authenticator and into the new datastore for the new authenticator while minimizing the impact on the user experience, thereby allowing transitioning from one authenticator to the next for the protection of web resources with minimal impact to applications or users. Blakely does not address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and does not teach or suggest the solution disclosed in the present application.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that locates the corresponding identification in the target datastore **and determines whether the target datastore includes a password associated with the identification.**

II. Blakely does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that submits the received identification and received password to the source user authenticator if the target datastore does not include a password associated with the identification.

Claim 1 also recites, "A method for migrating from a source user authenticator ... to a target user authenticator ... comprising ... If the target datastore does not include a password associated with the identification, then submit the received identification and received password to the source user authenticator."

The Office Action appears to suggest that the authentication step described in Mehring

discloses submitting the received identification and received password to the source user **if** the target data store does not include a password associated with the identification. However, as stated earlier, Mehring does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator. Instead, Mehring describes a method for allowing a remote system user to requests multiple software applications using a single log-in. More importantly, as stated in the section of Mehring cited in the Office Action (Col. 10., line 49 – Col. 11, line 10), although the remote user is only required to log-in once, the user information stored in the web browser log-in cache is submitted to the policy server every time the remote user logs-in to a different web server. Therefore, having user information stored in the web browser log-in cache does not eliminate the need to submit the user information to the policy server every time the remote user logs-in to a different web server. It only eliminates the need of having the remote user log-in separately to different web servers. By contrast, in the present application, once a password is associated with an identification in the target datastore, there is no longer a need to submit the request to the source user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest a method for migrating from a source user authenticator to a target user authenticator that submits the received identification and received password to the source user authenticator **if** the target datastore does not include a password associated with the identification.

III. The system and method of the present application populates the target datastore with the received password from the user. It does not populate the target datastore with the data from the source user authenticator.

Claim 1 further recites, “A method for migrating from a source user authenticator ... to a target user authenticator ... comprising ... On receipt of an approval response from the source user authenticator, populate the target datastore with the received password associating the received password with the corresponding identification.”

The Office Action noted that Blakely does not disclose this element. However, the Office Action suggested that:

It would have been obvious to one having ordinary skill in the art at the time of the invention was made to on receipt of an approval response from the source user authenticator populate the target datastore with the received password associating the received password with the corresponding identification, since it is known in

the art to facilitate the complete transfer of data, when data is found missing from the original source, it is restored by the data from the original source. (Page 5.)

Applicants are unclear as to how data can be restored from the original source if it is missing from the original source. If the Office Action is suggesting that the target datastore of the present application is populated from the source datastore, Applicants respectfully submit that this understanding is incorrect. For the reasons stated earlier, the target datastores cannot be populated from the source datastore because simply propagating passwords from one datastore to another is not possible when migrating from one vendor's proprietary database schema to another vendor's product due to the custom nature of some of the schema and the various encryption efforts. That is why it is necessary to receive the identification and the password from the user and not the source datastore. The system and method of the present application waits for the approval response from the source user authenticator before populating the target datastore with the identification and password entered by the user as a way of verifying if the identification and password entered by the user are valid, not as a way of restoring missing data.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor's proprietary database schema to another vendor's product and do not teach or suggest the solution disclosed in the present application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

IV. The agency module 112 of Mehring provides an interface for communications between the web server 110 and the policy server 114. It does not intercept a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

With regard to independent Claim 16, Claim 16 recites, "intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator."

The Office Action appears to suggest that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator. However, Mehring relates to a method of allowing a remote system user to requests multiple software applications using a single log-in. Mehring does not teach or suggest migrating data from a source datastore to a target datastore. Therefore, it cannot be said

that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator when Mehring does not teach or suggest a source user authenticator or a target user authenticator. Rather, “The agency module 112 provides an interface for communications between the web server 110 and the policy server 114.” (Col. 8, lines 6-8.) Providing an interface for communications between a web server and a policy server is not the same thing as intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Claim 16 also recites, “locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.”

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, as stated earlier, it is not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because the datastores of Blakely are configured to be propagated immediately with any changes to passwords in the DCE datastore.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.

Claim 16 further recites, “if the target datastore does not include a password associated with the identification, then: allowing the original intercepted request to go through to the source user authenticator.”

The Office Action does not appear to address this element of Claim 16, and Applicants are unable to find such a teaching in any of the cited references.

Accordingly, Applicants respectfully submit that none of the cited references, singly or in any motivated combination thereof, teaches or suggests that if the target datastore does not include a password associated with the identification, then allowing the original intercepted request to go through to the source user authenticator.

Claim 16 also recites, “on receipt of an approval response from the source user authenticator, populate the target datastore with the received password associating the received password with the corresponding identification.”

As stated earlier, the Office Action appears to suggest that the target datastore of the present application is populated from the source datastore. However, for the reasons stated earlier, the target datastores cannot be populated from the source datastore because simply propagating passwords from one datastore to another is not possible when migrating from one vendor’s proprietary database schema to another vendor’s product due to the custom nature of some of the schema and the various encryption efforts.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor’s proprietary database schema to another vendor’s product and do not teach or suggest the solution disclosed in the present application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

With regard to independent Claim 19, Claim 19 recites, “intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.”

The Office Action appears to suggest that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator. However, as stated earlier, the agency module 112 provides an interface for communications between the web server 110 and the policy server 114. (Col. 8, lines 6-8.) It does not intercept a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Claim 19 also recites, “locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.”

The Office Action appears to suggest that the foreign registries of Blakely locate a

corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, as stated earlier, it is not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because the datastores of Blakely are configured to be propagated immediately with any changes to passwords in the DCE datastore.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.

With regard to independent Claim 22, Claim 22 recites, “intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.”

The Office Action appears to suggest that the agency module 112 of Mehring intercepts a request to the source user authenticator from a user seeking access to information protected by the target user authenticator. However, as stated earlier, the agency module 112 provides an interface for communications between the web server 110 and the policy server 114. (Col. 8, lines 6-8.) It does not intercept a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Accordingly, Applicants respectfully submit that Mehring does not teach or suggest intercepting a request to the source user authenticator from a user seeking access to information protected by the target user authenticator.

Claim 22 also recites, “locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.”

The Office Action appears to suggest that the foreign registries of Blakely locate a corresponding identification in their target datastore and determine whether their datastores include a password associated with the identification. However, as stated earlier, it is not necessary for the foreign datastores of Blakely to determine if their datastores include a password associated with an identification because the datastores of Blakely are configured to be propagated immediately with any changes to passwords in the DCE datastore.

Accordingly, Applicants respectfully submit that Blakely does not teach or suggest

locating the corresponding identification in the target datastore and determining whether the target datastore includes a password associated with the identification.

Claim 22 also recites, “if the target datastore does not include a password associated with the identification, then: allowing the original intercepted request to go through to the source user authenticator.”

The Office Action does not appear to address this element of Claim 22, and Applicants are unable to find such a teaching in any of the cited references.

Accordingly, Applicants respectfully submit that none of the cited references, singly or in any motivated combination thereof, teaches or suggests that if the target datastore does not include a password associated with the identification, then allowing the original intercepted request to go through to the source user authenticator.

Claim 22 further recites, “on receipt of an approval response from the source user authenticator, capturing the password provided by the user in response to the source authenticator prompting and using the captured password as the received password.”

As stated earlier, the Office Action appears to suggest that the target datastore of the present application is populated from the source datastore. However, for the reasons stated earlier, the target datastores cannot be populated from the source datastore because simply propagating passwords from one datastore to another is not possible when migrating from one vendor’s proprietary database schema to another vendor’s product due to the custom nature of some of the schema and the various encryption efforts.

Neither of the cited references, singly or in any motivated combination thereof, address the problems associated with migrating data from one vendor’s proprietary database schema to another vendor’s product and do not teach or suggest the solution disclosed in the present application. Accordingly, Applicants respectfully submit that the teachings of these references would not suggest the claimed subject matter to a person of ordinary skill in the art.

Dependent Claims 2-15, 17, 18, 20, 21, 23, and 24 depend directly or indirectly from independent Claims 1, 16, 19, and 22 and incorporate all of the limitations thereof. Accordingly, for the reasons established above, Applicant respectfully submits that Claims 1-24 are not obvious in light of the suggested combination and respectfully request allowance of these claims.

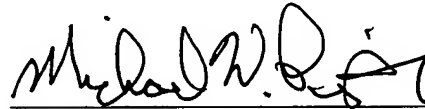
Conclusion

Applicants respectfully submit that the present application is in condition for full allowance for the reasons stated above, and Applicants respectfully request such allowance. If the Examiner has any questions or comments or feels it would be helpful in expediting the application, the Examiner is encouraged to telephone the undersigned at (972) 731-2288. This correspondence is intended to be a complete response to the Office Action dated January 23, 2006. The Commissioner is hereby authorized to charge payment of any further fees associated with any of the foregoing papers submitted herewith, or to credit any overpayment thereof, to Deposit Account No. 21-0765, Sprint.

Respectfully submitted,

Date: 4/24/2006

CONLEY ROSE, P.C.
5700 Granite Parkway, Suite 330
Plano, Texas 75024
(972) 731-2288
(972) 731-2289 (facsimile)



Michael W. Piper
Reg. No. 39,800

ATTORNEY FOR APPLICANT